

AMENDMENT TO SPECIFICATION

1. Please substitute the following amended title for the pending title on page 2, beginning on line 1 and ending on line 2, as follows:

[A] ~~CRYPTOGRAPHIC COMPUTATION USING MASKING TO PREVENT DIFFERENTIAL POWER ANALYSIS AND OTHER ATTACKS~~

2. Please substitute the following amended paragraph for the pending two paragraphs on page 2, beginning on line 4 and ending on line 7, as follows:

A2
This application is a continuation of U.S. Application No. 09/324,798, filed June 3, 1999, ^{now U.S. Pat. No. 6,278,783} (which is hereby incorporated by reference in its entirety), which claims the benefit of U.S. Provisional Application No. 60/087,826, filed June 3, 1998. U.S. Application No. 09/324,798 is related to co-pending U.S. Application No. 09/224,682, filed December 31, 1998.

[** Remainder of Page Is Intentionally Left Blank **]

A

**VERSION OF AMENDED SPECIFICATION
WITH MARKINGS TO SHOW CHANGES MADE**

1. The title on page 2, beginning on line 1 and ending on line 2, has been amended as follows:

**[IMPROVED DES AND OTHER] CRYPTOGRAPHIC [PROCESSES WITH
LEAK MINIMIZATION FOR SMARTCARDS AND OTHER
CRYPTOSYSTEMS] COMPUTATION USING MASKING TO PREVENT
DIFFERENTIAL POWER ANALYSIS AND OTHER ATTACKS**

2. The paragraphs on page 2, beginning on line 4 and ending on line 7, have been amended as follows:

This application is a continuation of U.S. Application No. 09/324,798, filed June 3, 1999 (which is hereby incorporated by reference in its entirety), which claims the benefit of U.S. [provisional patent application no.] Provisional Application No. 60/087,826, filed [on] June 3, 1998. [This application] U.S. Application No. 09/324,798 is related to co-pending U.S. [patent application no.] Application No. 09/224,682, filed [on] December 31, 1998.

**** Remainder of Page Is Intentionally Left Blank ****

53288.01-Palo Alto Server 1A

A